How Engineers Really Think About Risk: A Study of JPL Engineers

Dr. Jairus Hihn
Jet Propulsion Laboratory, California Institute of Technology

Deb Chattopadhyay
Jet Propulsion Laboratory, California Institute of Technology

Dr. Ricardo Valerdi
Massachusetts Institute of Technology

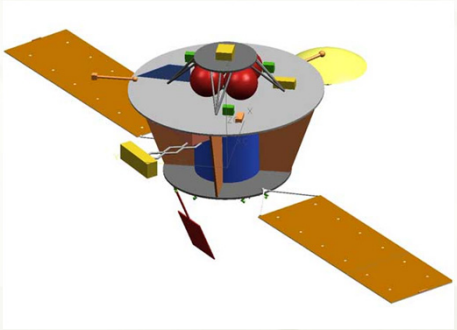
March 16, 2011

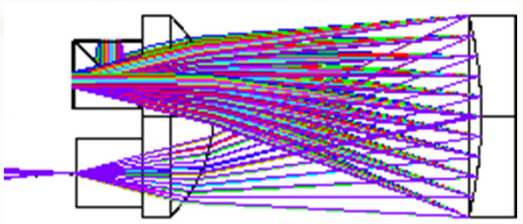
Outline

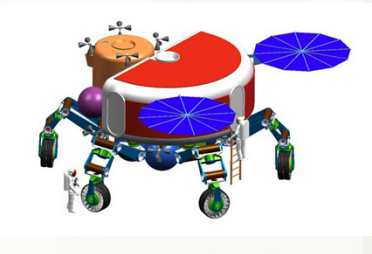
- Objectives
- Background
- Risk process in concurrent engineering
- Role of mental models in risk identification
- Methodology for capturing mental models
- Preliminary results
- Implications & next steps

Objectives

- To improve risk assessment practices as used during the mission design process by JPL's concurrent engineering teams
  - Developing effective ways to identify and assess mission risks
  - Providing a process for more effective dialog between stakeholders about the existence and severity of mission risks
  - Enabling the analysis of interactions of risks across concurrent engineering roles







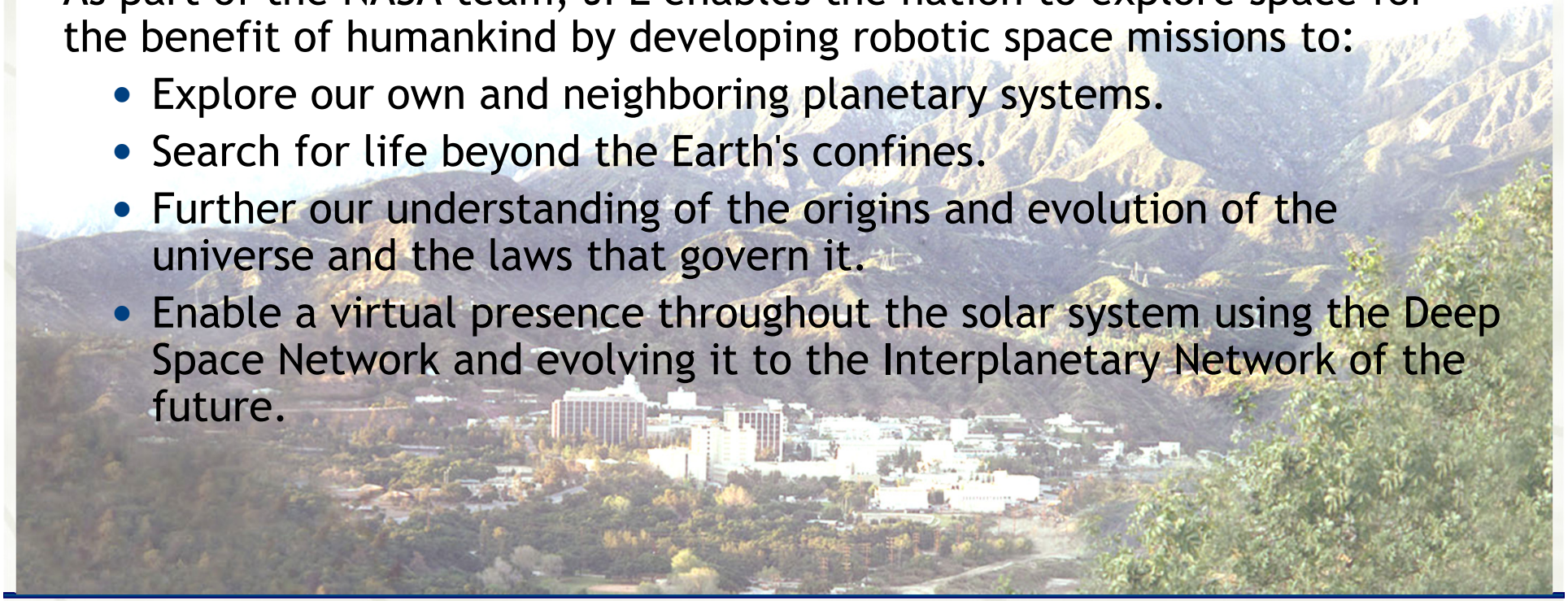
Background

The Jet Propulsion Laboratory is a Federally Funded Research & Development Center operated by the California Institute of Technology for the National Aeronautics and Space Administration.

- JPL has around 5000 employees and ~1.8 $B

As part of the NASA team, JPL enables the nation to explore space for the benefit of humankind by developing robotic space missions to:

- Explore our own and neighboring planetary systems.
- Search for life beyond the Earth's confines.
- Further our understanding of the origins and evolution of the universe and the laws that govern it.
- Enable a virtual presence throughout the solar system using the Deep Space Network and evolving it to the Interplanetary Network of the future.



What is Team X?

- Team X is JPL's Concurrent Engineering method* to support formulation-phase concept development
  - Rapid, responsive studies of architectures, missions, systems, and instruments
  - Rooted in our institutional experience building and operating flight systems
  - Created in April 1995
  - Over 1000 completed studies to date
  - Emulated by many institutions

* *Concurrent Engineering means:*

Diverse specialists working simultaneously, in the same place, with shared data, to yield an integrated design

When is Team X Work Applicable?

Find the Water!

Idea!

Formulation: We Are Here

Team X

Proposals

Project Development Timeline

Project Definition

Preliminary Design

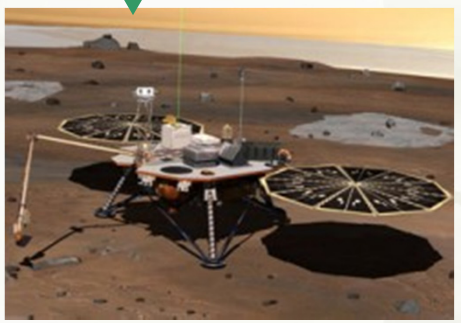
Design & Fabrication

Project Integration & Testing

Mission Operations

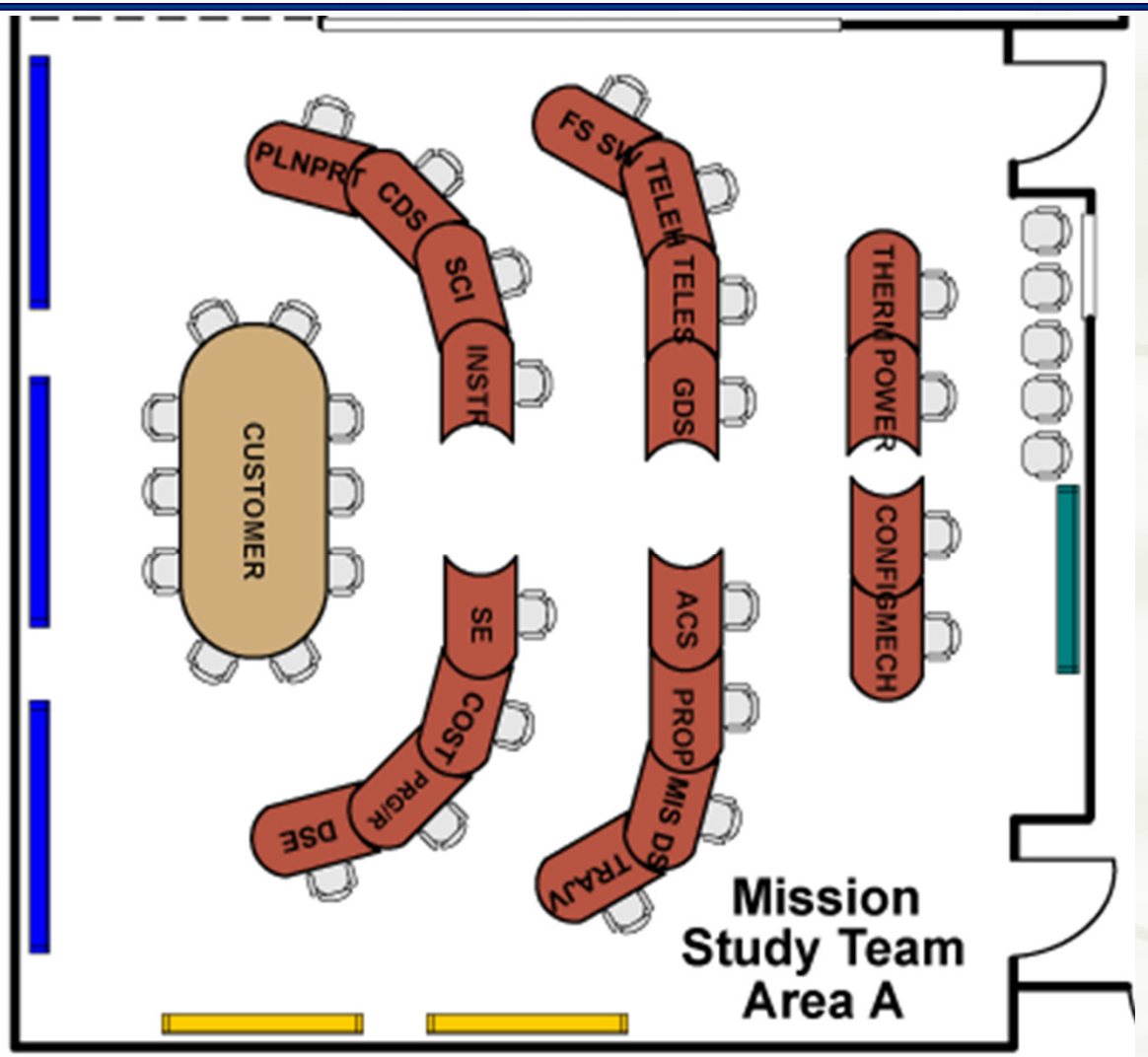
Phase A	Phase B	Phase C	Phase D	Phase E

Launch!



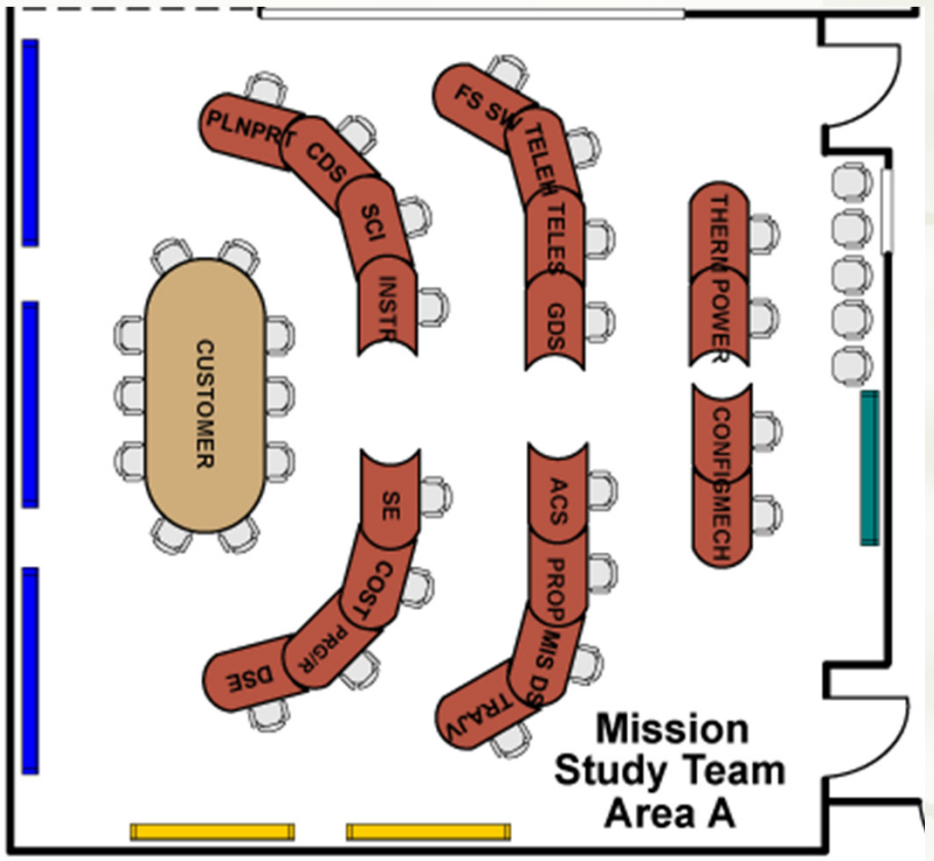
A Team of Experts

- Study Lead
- Systems Engineer
- Science
- Instruments
- Mission Design
- Trajectory & Visualization
- Configuration
- Power
- Propulsion
- Mechanical
- Thermal
- Attitude Control systems
- Command and Data Systems
- Telecom Systems
- Flight Software
- Ground Data Systems
- Programmatics / Risk
- Cost
- Domain Specialists as needed
  - Electronics
  - Optics
  - Detectors



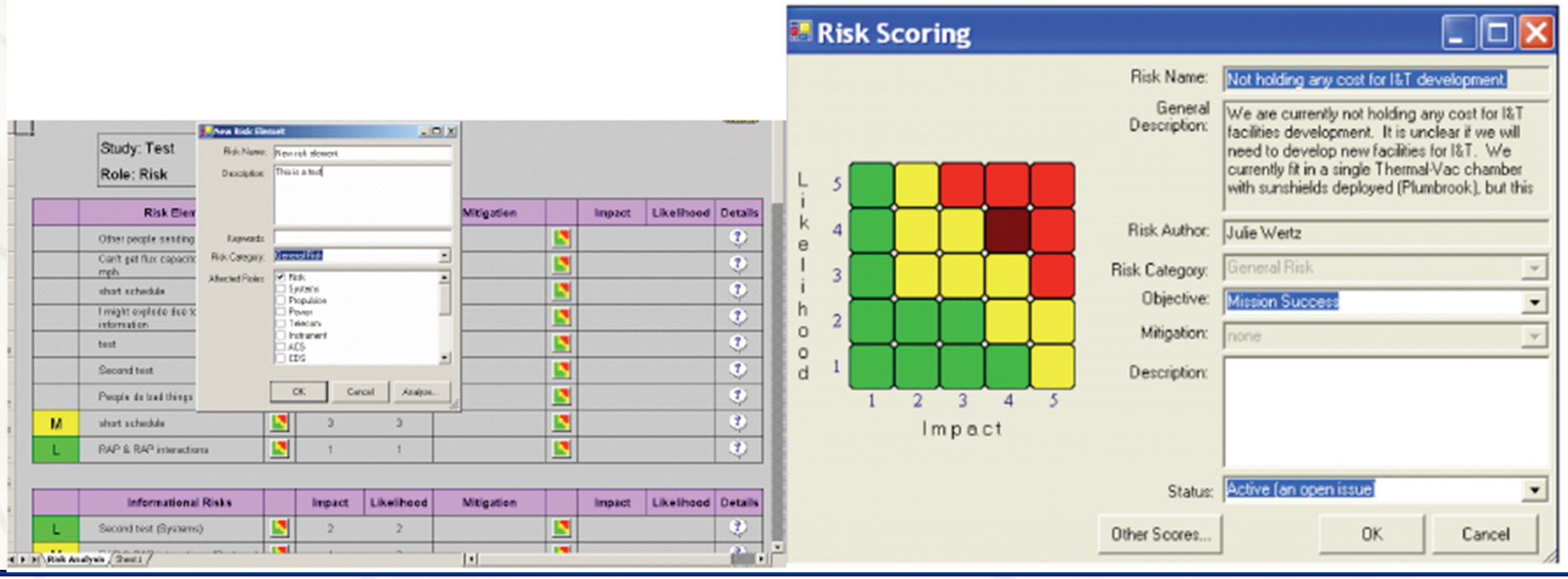
Risk Chair in Concurrent Engineering

- Risk Chair is responsible for
  - Study Risk Report
  - System level risks
  - Ensuring that the subsystem chairs respond to system risks and generate subsystem level risks
  - Risk Process and Infrastructure



Risk Tools in Concurrent Engineering

- Risk & Rationale Assessment Program (RAP)
- Enables risk identification & assessment
- Captures possible mitigations
- Supports cross chair communication
- But there are issues



Overview of Risk in a Concurrent Engineering Team

- **Risk process is highly subjective**
- **Limited data available to drive scoring**
- **Dependent on the person sitting in the risk chair**
- **Risk in a concurrent engineering team is very different from risk on a project**
  - Focus is on risk identification and initial assessment not risk management
- **In many cases the identified ‘risk’ item is primarily an issue that needs to be addressed in a proposal or analyzed further**
  - Less precise because driven by limited time to determine the answer
  - Difficult to use the standard techniques

Risk Checklists

Example Telecom

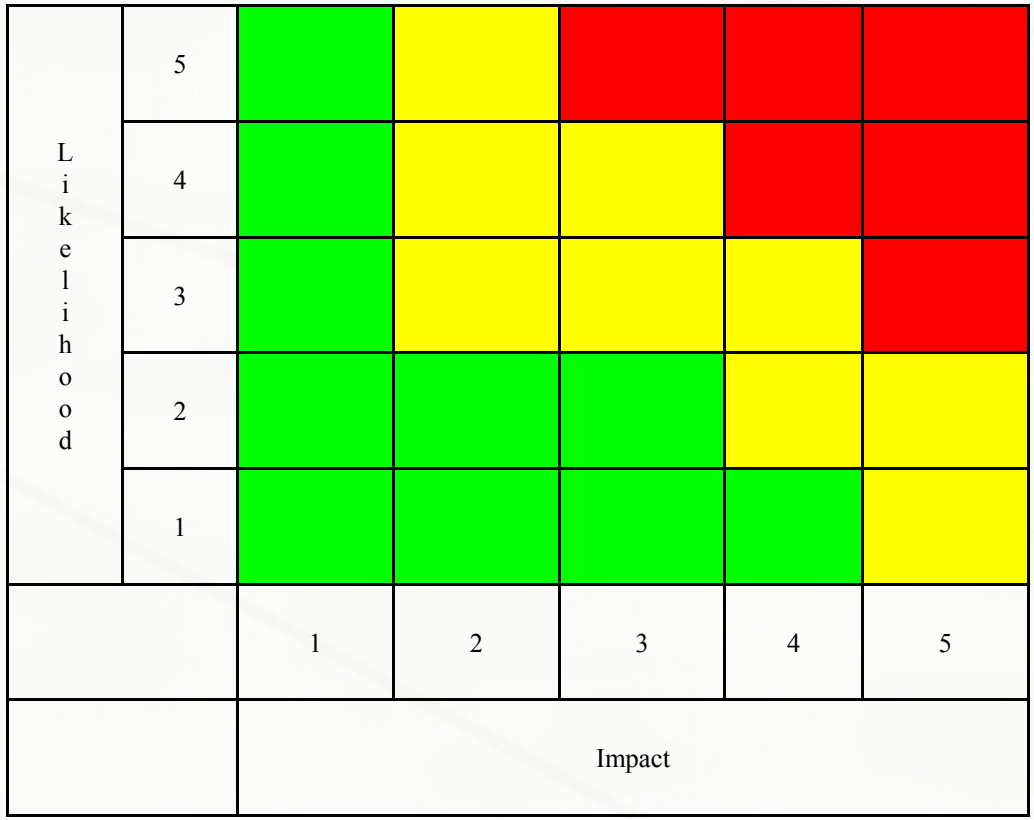
	Present?	Implementation	Mission	Examples
General Subsystem Risks				
Organizational				
Outside development of mission parts/contractor relations				This is applicable, one main contractor but sometimes others for radios
Technology Development and Heritage				
Low TRL /New Technology				
Technology inheritance from future missions				
Optimistic heritage assumptions				
Reliance on availability of residual hardware (such as Galileo heat shield, or SEP from DAWN)				
Parts Obsolescence				example of an older relay radio
Redundancy/Critical Failure				
Lack of Redundancy				
Dependencies on other flight systems within the mission				Potential failure of communication relay spacecraft
Inability to test certain components in a relevant environment				example of astromesh antennas
Very long mission (impact on component reliability)				
Environmental				
Harsh environment				example of Saturn probe with atmospheric effects
Unknown environment				example of unknown propagation medium
Environmental effects on antenna gain patterns				example for low gain, low frequency antennas that surrounding structures could change the antenna pattern
				M b bl d i h

Example Risk Checklist: Telecom (cont.)

Subsystem Specific				
High data rates				
Deployable Antenna				example of Galileo high gain antenna
Insufficient communication during mission critical events				
Communication coverage for safe modes				example of losing attitude control and still being able to communicate, if there are limits it may be a risk
Spectrum limits or interference risk				examples include possibility of not receiving large enough bandwidth allocation or having multiple spacecraft on the same channel
Needed hardware capability not currently available				example of assuming that a supplier can change the modulation scheme of a radio
Requirement of always keeping transmitter on is not satisfied				This is a design principle but often violated

Risk Scoring

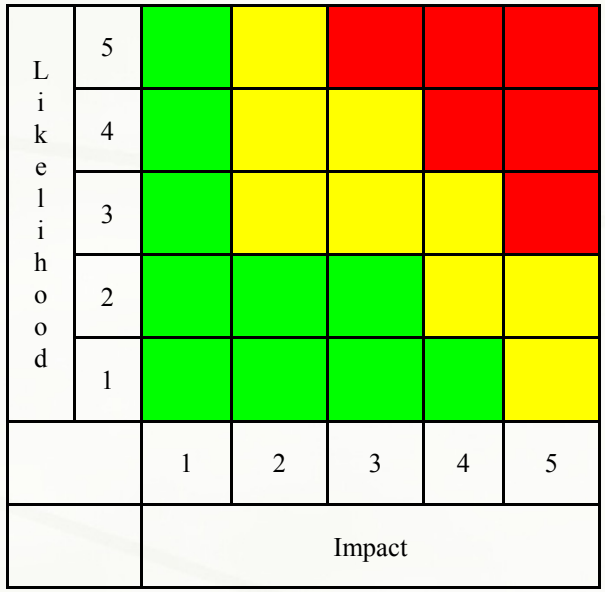
What is a 1,1 Risk?



Commonly Used Risk Scoring Guidance

Likelihood of occurrence

- Very High (>10%)
- High (>5%)
- Medium (>1%)
- Low (>0.5%)
- Very Low (>0.1%)



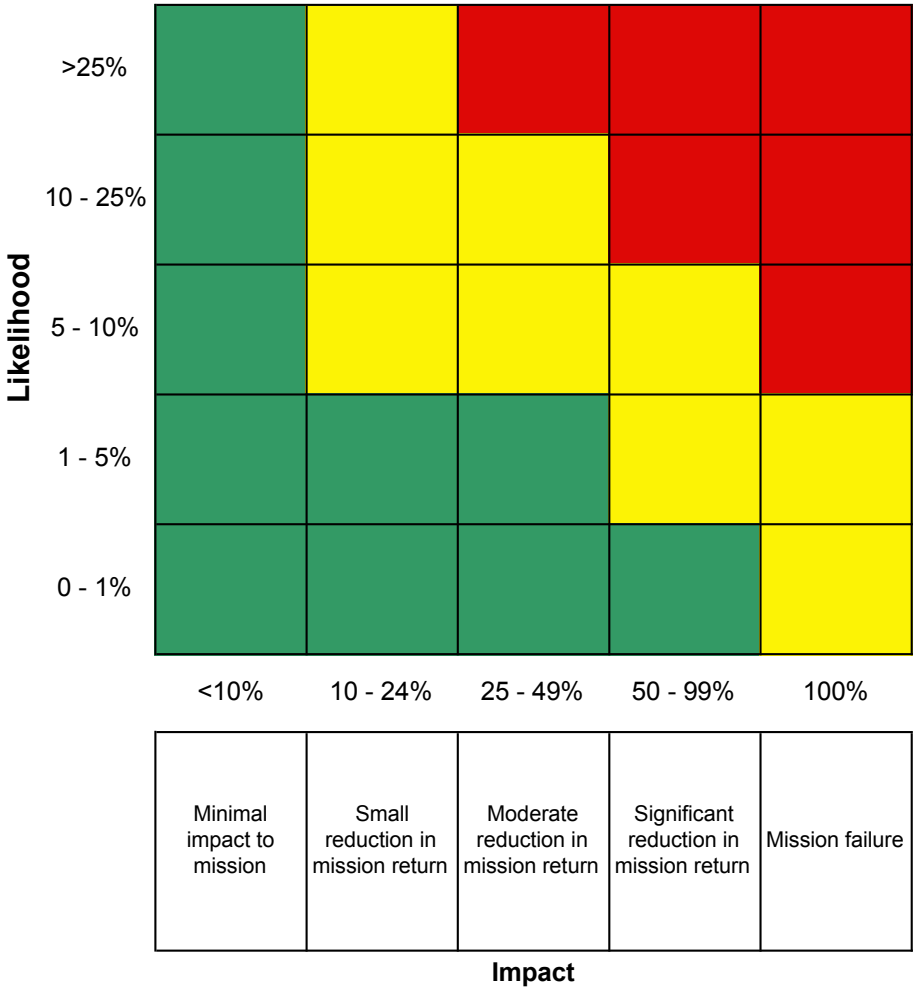
Loss of mission objectives

- Mission Failure (100%)
- Significant (90%)
- Moderate (50%)
- Small (10%)
- Minimal (1%)

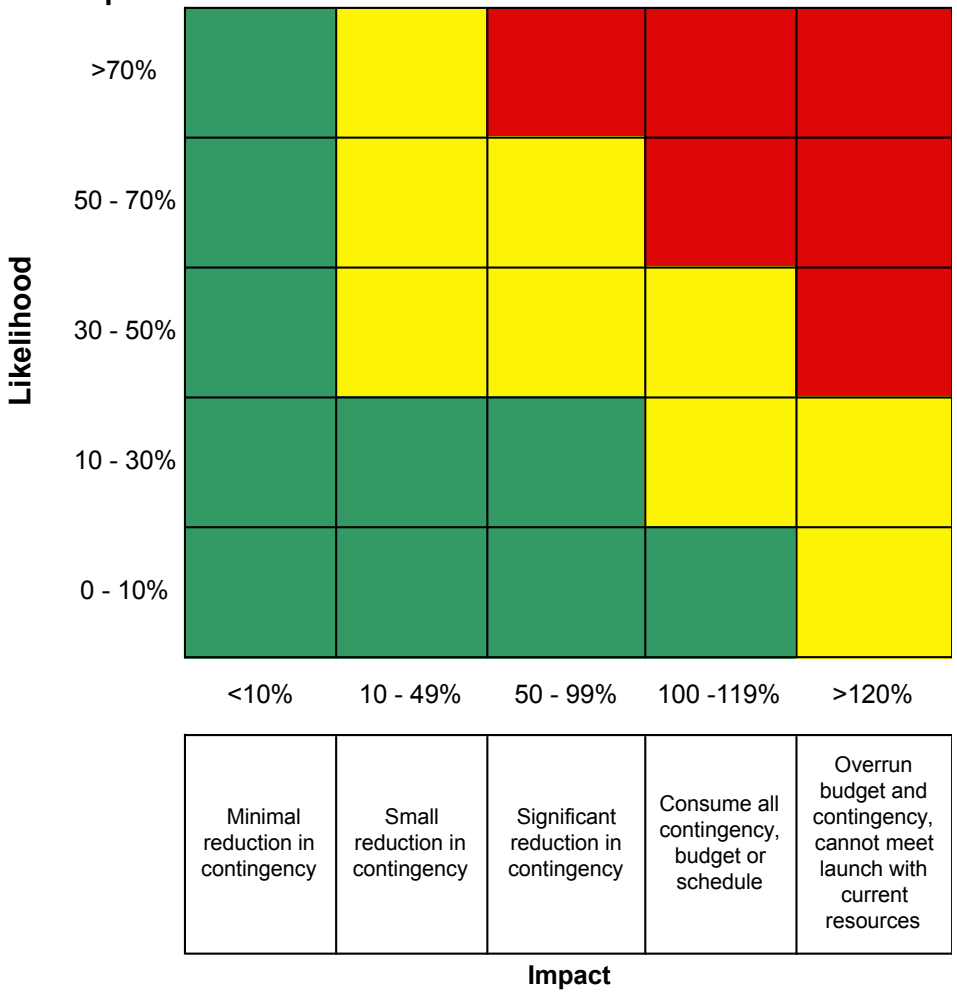
New Risk Scoring Guidance

- Translation of impact and likelihood ratings into Red-Yellow-Green for NASA 5x5 risk matrix

Mission Risk:



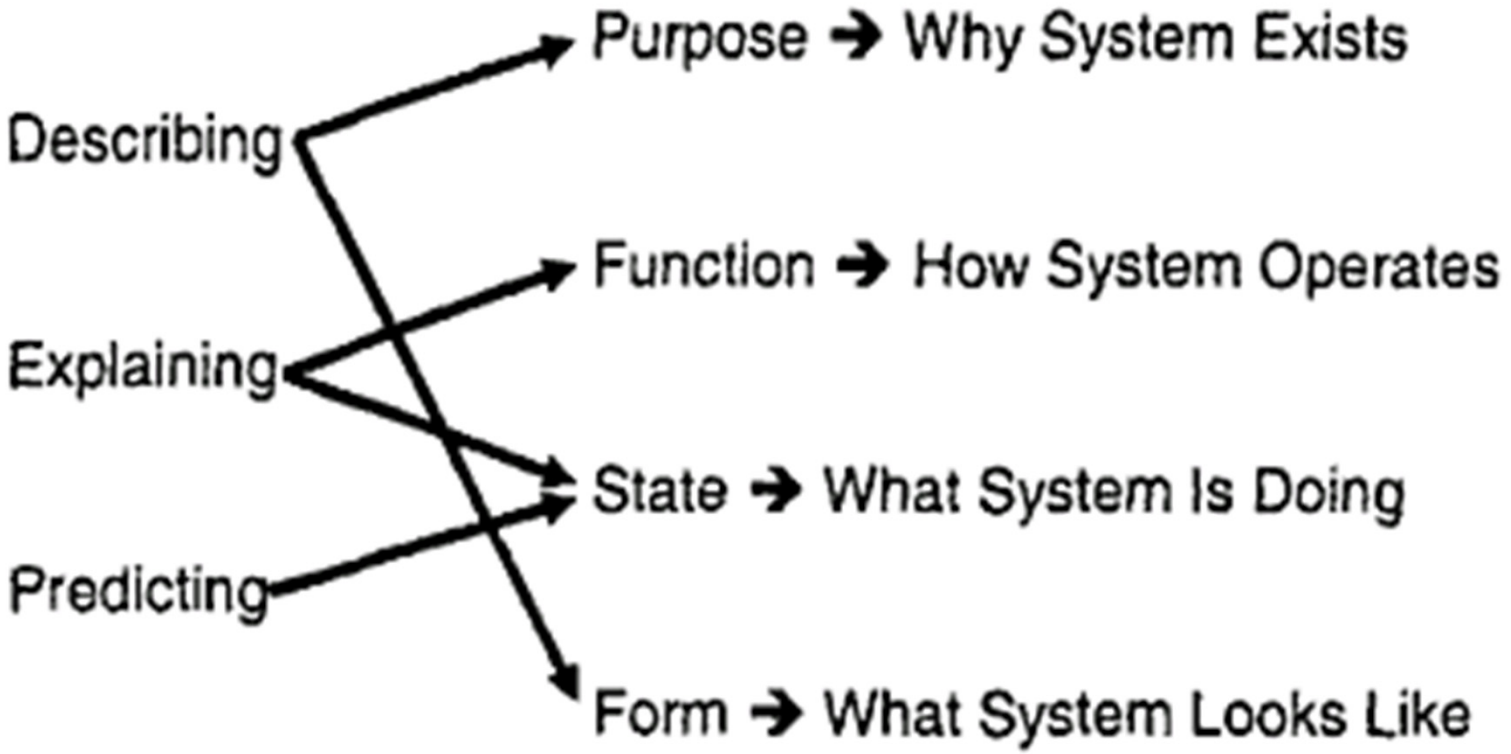
Implementation Risk:



Role of Mental Models in Risk Identification

Mental models are psychological representations of real, hypothetical or imaginary situations

(Craik, K. The Nature of Explanation, 1943)

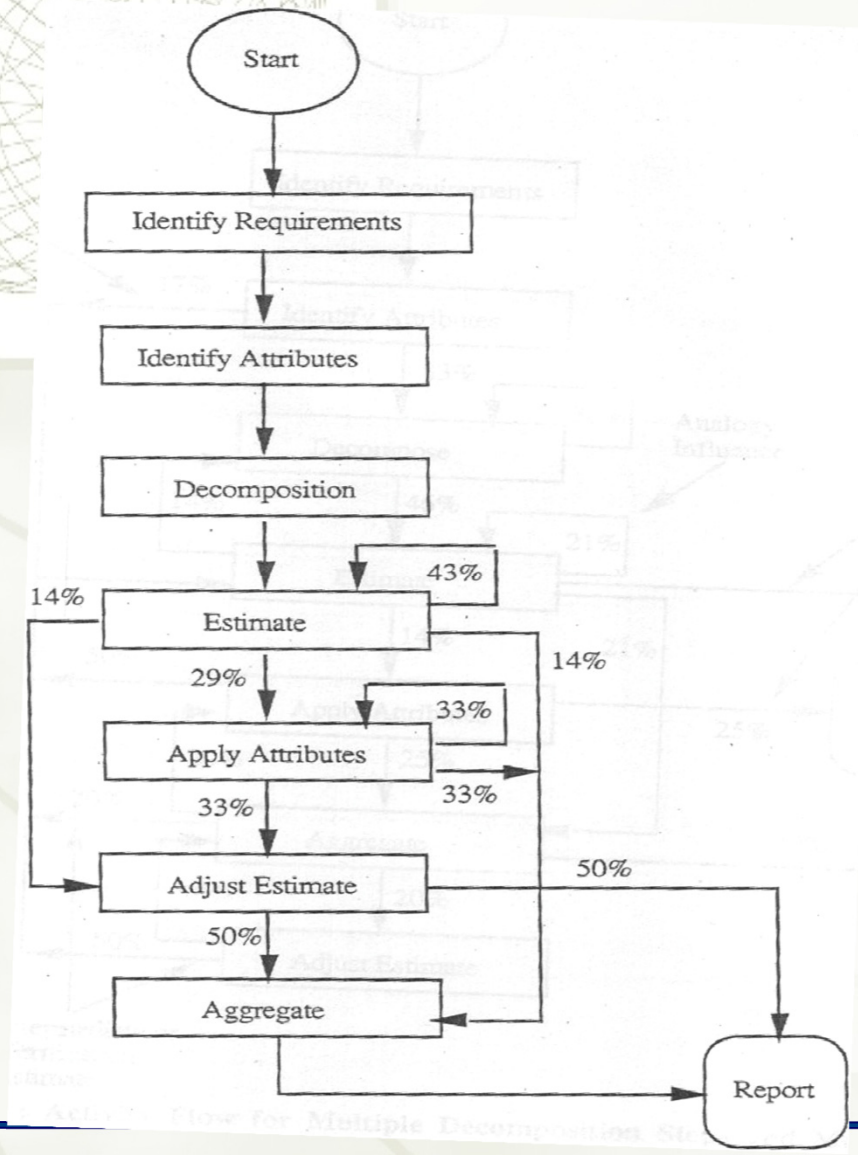


Rouse, W. B., People and organizations: explorations of human-centered design , Wiley 2007.

Methodology for Capturing Mental Models

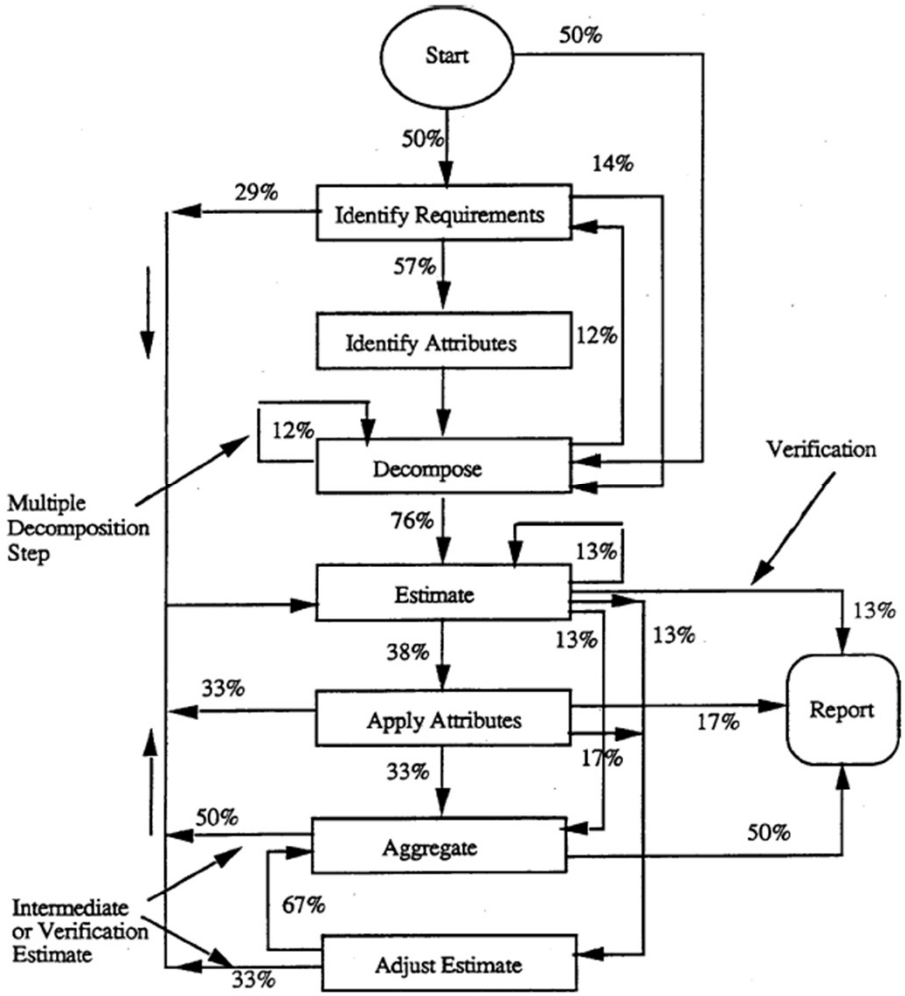
- Protocol analysis is a technique for converting unstructured and semi-structured self reported narratives (verbal protocols) into data describing cognitive processes
- Developed by Ericson, K. and Simon, H., Protocol Analysis, MIT press, 1984
- The most important step in the data analysis is the construction of a scoring taxonomy which captures all the relevant characteristics
- Requires three people to score the data
  - Two for the initial scoring and the third to settle differences

Example of a Model Based Cost Estimation Mental Model



Software Forecasting As it Is Really Done: A Study of JPL Software Engineers. **Proceedings of the Eighteenth Annual Software Engineering Workshop**. Goddard Space Flight Center. December 1-2, 1993, Griesel, A., Hihn, J., Bruno, K., Fouser, T., and Tausworthe, R..

Example of a Judgment Based Cost Estimation Mental Model



Methodology for Capturing Risk Mental Models

- Semi-structured interviews intended to capture reasoning behind experts' actions

  - What triggers you to identify something as a risk?
  - What is your personal checklist for determining whether something is a risk?
  - What do you think about when you provide a scoring for each risk?
  - Do you start with the colors or the numbers to assess risk probability and impact on a matrix?
  - What are the sources of information for uncertainty/risk?

Overview of Key Findings

- **General**
  - Some chairs lead risk identification (e.g. Instruments) and some chairs are more reactive (GDS)
    - How they approach risk is very different

- **Risk in a concurrent engineering team is very different from risk on a project**
  - Less precise because driven by time to determine the answer
  - Limited data available to drive scoring
  - Cannot use many of the standard techniques

- **Risk Documentation**
  - Risk are not specified completely contributing to inconsistency
    - Sometimes the chair describes the cause and sometimes the effect
    - Sometimes only the name of the ‘element’ is used with minimal to no description
  - Value of reviewing and rewriting risks outside of session for clarity and consistency

Overview of Key Findings: Risk Identification

- **Risk Identification**
  - In the early stages of the lifecycle it is difficult to distinguish between an Issue, Concern, or Risk
  - Everyone applies some type of risk threshold
    - Normal risks are not worth writing down as as they are part of the ‘risk’ of doing business
  - Risk identification is very dependent upon immediate experience. If a person is constantly involved in high-risk projects, their risk threshold may become higher than usual. If they were recently burned by a particular failure, they will overstate the existence of a related risk.

Overview of Key Findings: Risk Scoring

- **Scoring is a fuzzy hybrid of qualitative and quantitative assessment.**
  - Lynne Cooper describes risk assessment in the early life-cycle as 'pre-quantitative risk'.

- **Rather than thinking about risk quantitatively, engineers appear to have a better sense of levels of risk.**
  - A representation of the thought process might be:
    - This is something to keep an eye on (green risk)
    - This is something that I am very worried about and it could cause total mission loss (red risk)
    - This is something to worry about and it might be even worse than I realize since there is limited information currently available (yellow risk)

Risk Mental Models for Expert Engineers

- Expert engineer risk mental models
  - Include a focused mental checklist of a few questions
  - Repeatable systematic model with simple structure, leading to consistent risk identification in various settings

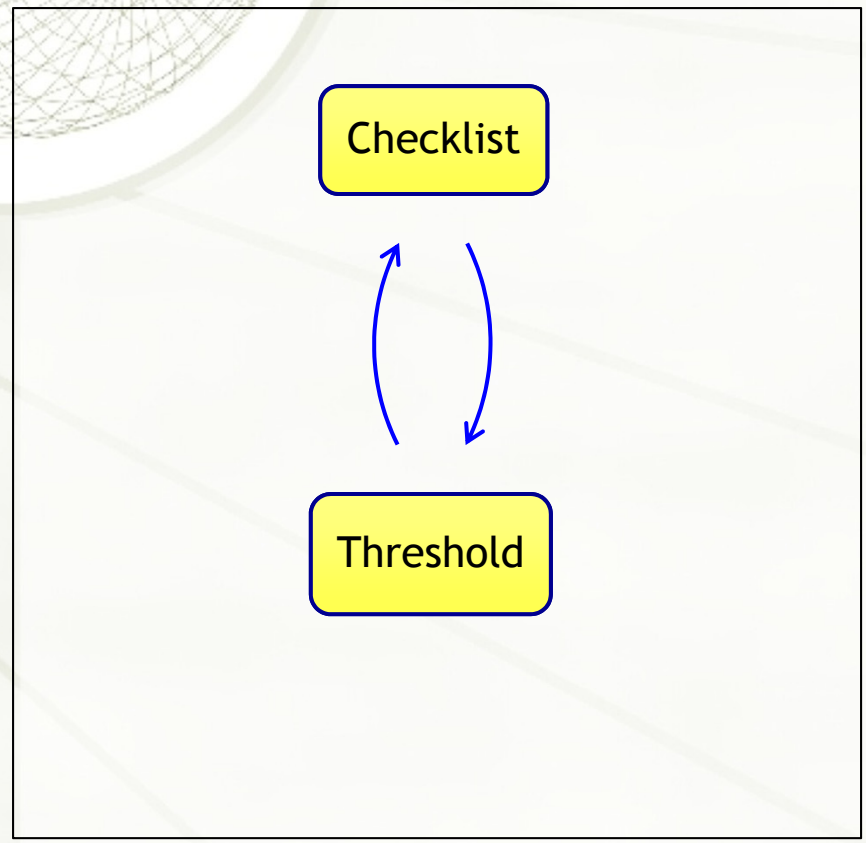
Mental Checklist	
ACS	Instrument
• How well do I need to know where I am? • How well do I have to point? • How do I meet the above requirements?	• Who *is building the mission?* • What *are they trying to do?* • Where *are they going?* • When *is the mission?* • Why *are they doing this?* • How *are they implementing it?* • How *much will it cost?*
If there is uncertainty about the answer to these questions above a personal threshold, an issue is noted.	

Attempt to reduce uncertainty by gathering information from people, databases and other external information sources.

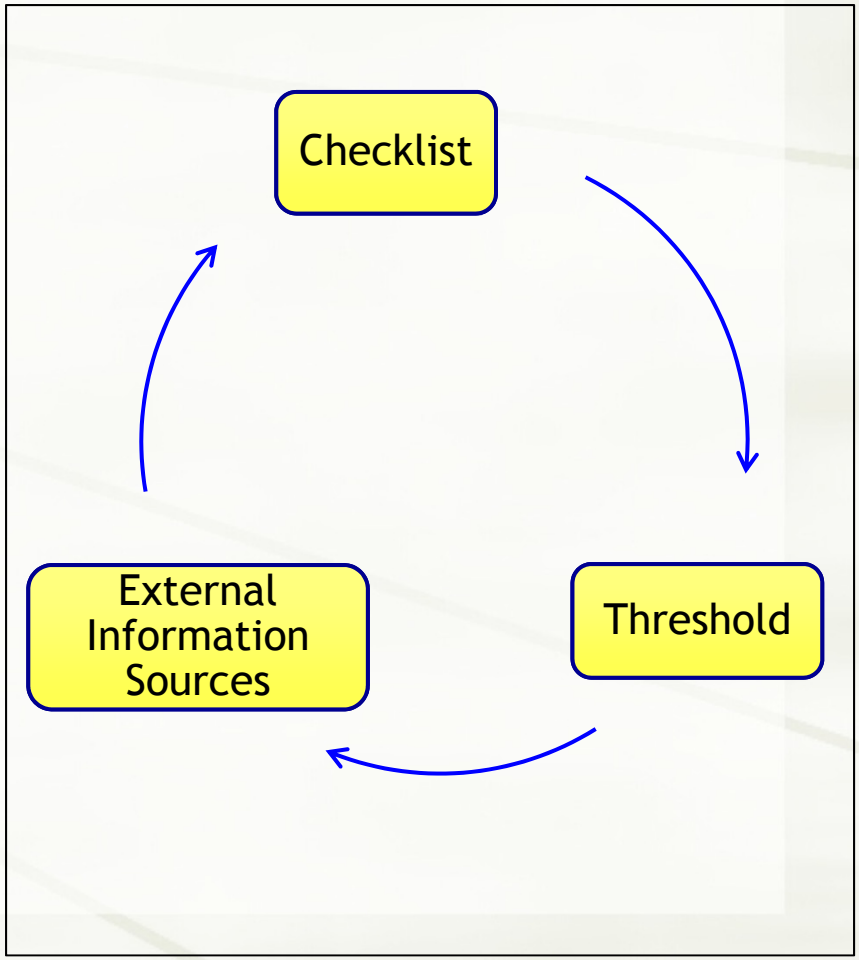
Uncertainty irreducible in given time or with given resources noted as **RISK**

Mental Model Loops

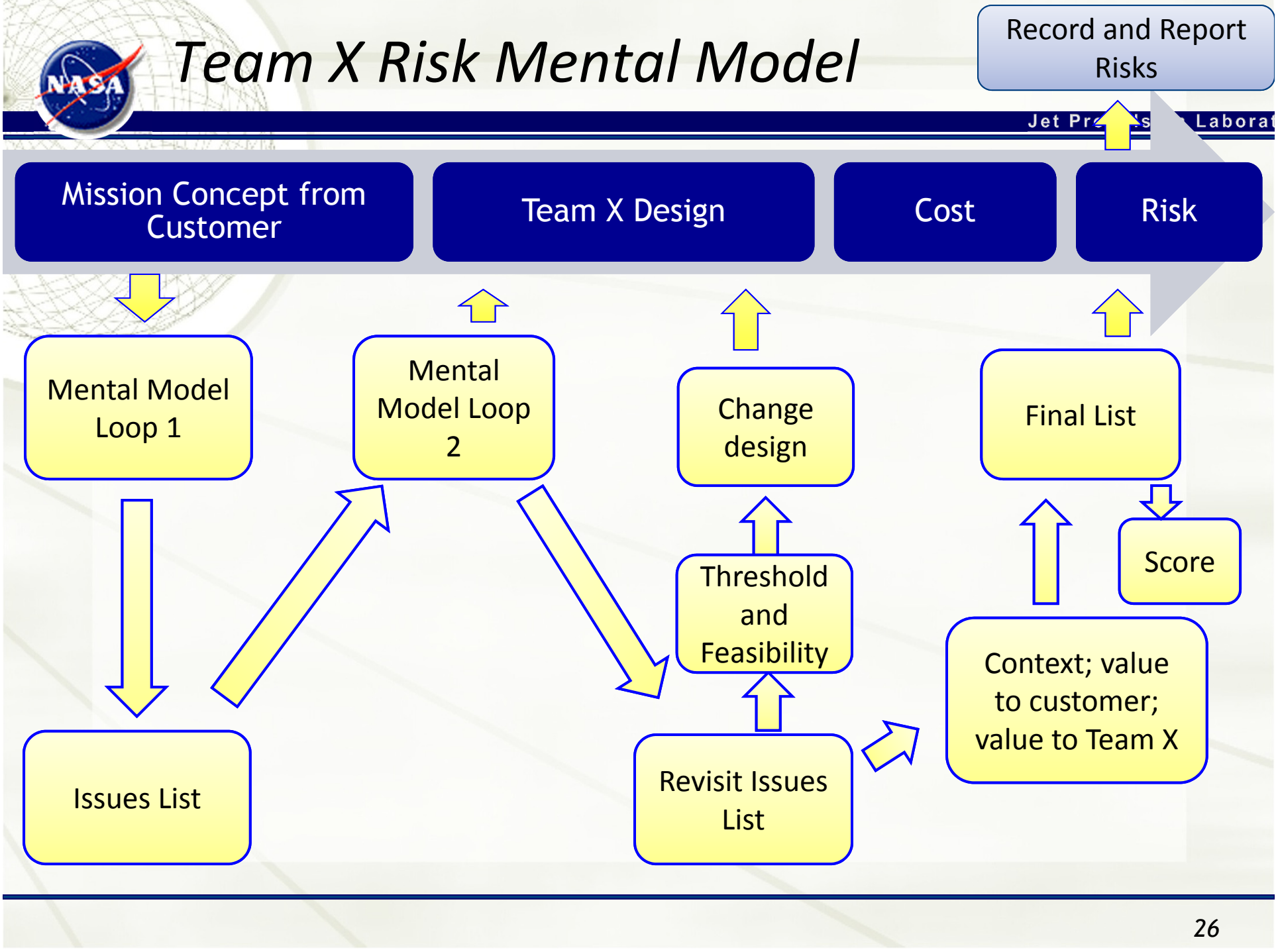
- **Mental Model Loop 1**



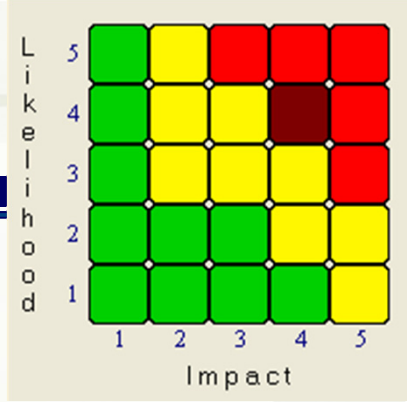
- **Mental Model Loop 2**



Team X Risk Mental Model



Conclusions etc.



- Need to focus on pre-quantitative risk
- Experts differ from novices
  - Experts have a repeatable mental model of risk, while novices have a more unpredictable models
  - Efficiently organize knowledge…clustered into related chunks…governed by generalizable principles
- Papers

  "Identification And Classification Of Common Risks In Space Science Missions", Jairus Hihn, Debarati Chattopadhyay, Robert Hanna, Daniel Port, Sabrina Eggleston, Proceedings AIAA Space 2010 Conference and Exposition, 1-3 September, Anaheim, CA.

  "Risk Identification and Visualization in a Concurrent Engineering Team Environment", Jairus Hihn, Debarati Chattopadhyay, Robert Shishko, Proceedings of the ISPA/SCEA 2010 Joint International Conference, June 8-11, 2010, San Diego, CA.